**Identificación de activos**

**……….**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | NOMBRE | DESCRIPCION | RESPONSABLE | TIPO |
| 01 | Correo electrónico | Correo de uso interno contratado a terceros para el intercambio electrónico de datos. | Director de Sistemas | Servicio |
| 02 | Internet | Servicio de uso interno contratado a terceros para el acceso a internet | Director de Sistemas | Servicio |
| 03 | Mensajería instantánea | Sistema de uso interno para acceso remoto e intercambio electrónico de datos. | Director de Sistemas | Servicio |
| 04 | Plan operativo | Documentación de interés para la administración y la gestión interna | Director de Sistemas | Datos / Información |
| 05 | Plan de contingencia informática | Documentación de interés para la administración y la gestión interna | Director de Sistemas | Datos / Información |
| 06 | Plan de mantenimiento preventivo y correctivo de equipos informáticos | Documentación de interés para la administración y la gestión interna | Director de Sistemas | Datos / Información |
| 07 | Programas informáticos diseñados por el GAD | Sistemas ejecutables de uso interno para desempeño de tareas del GAD. | Director de Sistemas | Datos / Información |
| 08 | Políticas y normas para el procedimiento de la operatividad y manejo de sistemas | Documentación de interés para la administración y la gestión interna | Director de Sistemas | Datos / Información |
| 09 | Inventario de función y asignación de equipos de computación | Documentación de interés para la administración y la gestión interna | Director de Sistemas | Datos / Información |
| 10 | Registro de equipos, materiales, herramientas y demás complementos informáticos | Documentación de interés para la administración y la gestión interna | Director de Sistemas | Datos / Información |
| 11 | Instructivo de cuidado y mantenimiento físico de los equipos y componentes informáticos | Documentación de interés para la administración y la gestión interna | Director de Sistemas | Datos / Información |
| 12 | Informes de ejecución de planes de la Dirección | Documentación de interés para la administración y la gestión interna | Director de Sistemas | Datos / Información |
| 13 | Inventario actualizado de hardware y software adquirido por el GAD | Documentación de interés para la administración y la gestión interna | Director de Sistemas | Datos / Información |
| 14 | Respaldos de información | Archivos electrónicos de interés para la administración y la gestión interna | Director de Sistemas | Datos / Información |
| 15 | Bases de datos | Archivos electrónicos de interés para la administración y la gestión interna | Director de Sistemas | Datos / Información |
| 16 | Windows Server | Sistema operativo de uso estándar para servidor de ficheros y aplicaciones | Director de Sistemas | Aplicaciones |
| 17 | Windows XP | Sistema operativo de uso estándar para servidor de aplicaciones y estaciones de trabajo | Director de Sistemas | Aplicaciones |
| 18 | Linux Centos | Sistema operativo de uso estándar para servidor de ficheros y aplicaciones | Director de Sistemas | Aplicaciones |
| 19 | BorgChat | Sistema de mensajería de uso estándar para intercambio de mensajes y archivos | Director de Sistemas | Aplicaciones |
| 20 | Kaspersky Business Space Security | Sistema antivirus de uso estándar para proteccion de ficheros y aplicaciones | Director de Sistemas | Aplicaciones |
| 21 | SAM (Control de ingresos) | Sistema informático desarrollado a la medida para uso interno | Director de Sistemas | Aplicaciones |
| 22 | PFG (Control de Archivos y Financiero) | Sistema informático desarrollado a la medida para uso interno | Director de Sistemas | Aplicaciones |
| 23 | OLYMPO (Control Contable y Presupuesto) | Sistema informático desarrollado a la medida para uso interno | Director de Sistemas | Aplicaciones |
| 24 | Control de Bodega y Proveedores | Sistema informático desarrollado a la medida para uso interno | Director de Sistemas | Aplicaciones |
| 25 | Control de Mercados | Sistema informático desarrollado a la medida para uso interno | Director de Sistemas | Aplicaciones |
| 26 | Servidor Principal | Equipo para el almacenamiento de datos | Director de Sistemas | Hardware |
| 27 | Servidor Financiero | Equipo para el almacenamiento de datos y sistemas distribuidos de aplicaciones | Director de Sistemas | Hardware |
| 28 | Servidor Alterno | Equipo para el almacenamiento de datos y sistemas distribuidos de aplicaciones | Director de Sistemas | Hardware |
| 29 | Servidor de Imágenes | Equipo para el almacenamiento de datos | Director de Sistemas | Hardware |
| 30 | Servidor de Control de Antivirus | Equipo para el almacenamiento de datos y sistemas distribuidos de aplicaciones | Director de Sistemas | Hardware |
| 31 | Servidor Proxy | Equipo para el almacenamiento de datos y acceso a internet | Director de Sistemas | Hardware |
| 32 | Switch | Equipo de soporte de red y comunicaciones | Director de Sistemas | Hardware |
| 33 | Router | Equipo de soporte de red y comunicaciones | Director de Sistemas | Hardware |
| 34 | Impresora / Scanner | Equipo periférico | Director de Sistemas | Hardware |
| 35 | Red Interna | Red de área local | Director de Sistemas | Redes de Comunicación |
| 36 | Pendrive | Dispositivo de almacenamiento masivo portable USB | Director de Sistemas | Soporte |
| 37 | Disco duro externo | Dispositivo de almacenamiento masivo portable USB | Director de Sistemas | Soporte |
| 38 | Sistema de Alimentación Ininterrumpida (UPS) | Fuente de alimentación eléctrica | Director de Sistemas | Equipamiento |
| 39 | Generador Eléctrico | Fuente de alimentación eléctrica | Director de Sistemas | Equipamiento |

Una vez identificados los activos se continua con la respectiva valoración, esta se la realiza en base a las características y atributos propio que tiene cada activo y le dan valor.

La valoración la realiza el Director de sistemas como encargado de los activos y conocedor del valor e importancia, pudiendo determinar así los principales activos que posee la Dirección de Sistemas.

Esta valoración se la realiza en base a las siguientes dimensiones o características propias que poseen los activos y el perjuicio que causaría su perdida.

**[ D ]** **Disponibilidad**: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?

**[ I ]** **Integridad**: ¿qué perjuicio causaría que estuviera dañado o corrupto?

**[ C ]** **Confidencialidad**: ¿qué daño causaría que lo conociera quien no debe?

**[ A\_S ]** **Autenticidad**: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa? Esta valoración es típica de servicios (autenticidad del usuario).

**[ A\_D ]** **Autenticidad**: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa? Esta valoración es típica de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar).

**[ T\_S ]** **Trazabilidad** del uso del **servicio**: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

**[ T\_D ]** **Trazabilidad** del acceso a los **datos**: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [S] Servicios | | | | | | | | |
| ID | **Activo** | **Dimensiones** | | | | | | |
| **[D]** | **[I]** | **[C]** | **[A\_S]** | **[A\_D]** | **[T\_S]** | **[T\_D]** |
| 01 | Correo electrónico | 7 |  |  | 8 |  | 9 |  |
| 02 | internet | 7 |  |  | 5 |  | 5 |  |
| 03 | Mensajería instantánea | 8 |  |  | 7 |  | 9 |  |

Tabla 3.3 Valoración de Servicios.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [D] Datos/Información | | | | | | | | |
| ID | **Activo** | **Dimensiones** | | | | | | |
| **[D]** | **[I]** | **[C]** | **[A\_S]** | **[A\_D]** | **[T\_S]** | **[T\_D]** |
| 04 | Plan operativo |  | 6 | 5 |  | 6 |  | 6 |
| 05 | Plan de contingencia informática |  | 8 | 5 |  | 7 |  | 7 |
| 06 | Plan de mantenimiento preventivo y correctivo de equipos informáticos |  | 6 | 5 |  | 6 |  | 6 |
| 07 | Programas informáticos diseñados por la institución |  | 8 | 8 |  | 7 |  | 7 |
| 08 | Políticas y normas para el procedimiento de la operatividad y manejo de sistemas informáticos |  | 6 | 5 |  | 6 |  | 6 |
| 09 | Inventario de distribución y asignación de equipos de computación |  | 6 | 5 |  | 6 |  | 6 |
| 10 | Registro de equipos, materiales, herramientas y demás complementos informáticos |  | 6 | 5 |  | 6 |  | 6 |
| 11 | Instructivos de cuidado y mantenimiento físico de los equipos y componentes informáticos |  | 6 | 5 |  | 6 |  | 6 |
| 12 | Informes de ejecución de planes de la dirección |  | 6 | 5 |  | 6 |  | 6 |
| 13 | Inventario actualizado de hardware y software adquirido por la municipalidad |  | 6 | 5 |  | 6 |  | 6 |
| 14 | Respaldos de información |  | 9 | 8 |  | 9 |  | 9 |
| 15 | Base de datos |  | 9 | 8 |  | 9 |  | 9 |

Tabla 3.4 Valoración de Datos/Información.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [SW] Aplicaciones (Software) | | | | | | | | |
| ID | **Activo** | **Dimensiones** | | | | | | |
| **[D]** | **[I]** | **[C]** | **[A\_S]** | **[A\_D]** | **[T\_S]** | **[T\_D]** |
| 16 | Windows Server | 9 | 8 | 8 |  |  |  |  |
| 17 | Windows XP Profesional | 8 | 8 | 7 |  |  |  |  |
| 18 | Linux Centos | 8 | 8 | 8 |  |  |  |  |
| 19 | Borgchat | 8 | 7 | 8 |  |  |  |  |
| 20 | Kaspersky Business Space Security | 8 | 8 | 8 |  |  |  |  |
| 21 | SAM (Control de ingresos) | 9 | 9 | 8 |  |  |  |  |
| 22 | PFG (Control de archivos y financiero) | 8 | 8 | 8 |  |  |  |  |
| 23 | OLYMPO (Control contable y presupuesto) | 8 | 8 | 8 |  |  |  |  |
| 24 | Control de bodega y proveedores | 6 | 6 | 7 |  |  |  |  |
| 25 | Control de mercados | 5 | 5 | 6 |  |  |  |  |

Tabla 3.5 Valoración de Aplicaciones.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [HW] Hardware | | | | | | | | |
| ID | **Activo** | **Dimensiones** | | | | | | |
| **[D]** | **[I]** | **[C]** | **[A\_S]** | **[A\_D]** | **[T\_S]** | **[T\_D]** |
| 26 | Servidor Principal | 9 | 8 | 8 |  |  |  |  |
| 27 | Servidor Financiero | 9 | 8 | 8 |  |  |  |  |
| 28 | Servidor Alterno | 8 | 7 | 7 |  |  |  |  |
| 29 | Servidor Imágenes | 9 | 8 | 8 |  |  |  |  |
| 30 | Servidor Control de antivirus | 8 | 8 | 8 |  |  |  |  |
| 31 | Servidor Proxy | 8 | 8 | 8 |  |  |  |  |
| 32 | Switch | 8 | 7 | 7 |  |  |  |  |
| 33 | Router | 8 | 7 | 7 |  |  |  |  |
| 34 | Impresora / Scanner | 5 | 5 | 3 |  |  |  |  |

Tabla 3.6 Valoración de Hardware.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [COM] Redes de comunicación | | | | | | | | |
| ID | **Activo** | **Dimensiones** | | | | | | |
| **[D]** | **[I]** | **[C]** | **[A\_S]** | **[A\_D]** | **[T\_S]** | **[T\_D]** |
| 35 | Red interna | 9 | 8 | 8 |  |  |  |  |

Tabla 3.7 Valoración de Redes de Comunicación.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [SI] Soporte de información | | | | | | | | |
| ID | **Activo** | **Dimensiones** | | | | | | |
| **[D]** | **[I]** | **[C]** | **[A\_S]** | **[A\_D]** | **[T\_S]** | **[T\_D]** |
| 36 | Pendrive | 7 | 7 | 7 |  |  |  |  |
| 37 | Disco duro portable | 8 | 9 | 9 |  |  |  |  |

Tabla 3.8 valoración de Soporte de Información.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [AUX] Equipamiento auxiliar | | | | | | | | |
| ID | **Activo** | **Dimensiones** | | | | | | |
| **[D]** | **[I]** | **[C]** | **[A\_S]** | **[A\_D]** | **[T\_S]** | **[T\_D]** |
| 38 | Sistema de alimentación ininterrumpida (UPS) | 5 | 5 | 3 |  |  |  |  |
| 39 | Generador eléctrico | 6 | 5 | 3 |  |  |  |  |

Tabla 3.9 Valoración de Equipamiento Auxiliar.

Con la valoración de los activos realizada, para continuar con el análisis de riesgo se tendrán en cuanta solamente aquellos activos que hayan alcanzado una calificación considerable y resalten sobre los demás.

Los activos fueron medidos en escala del 1 – 10 y para separar los más importantes se consideró los siguientes rangos de valoración:

* 10 Muy Alto
* 7 – 9 Alto
* 4 – 6 Medio
* 1 – 3 Bajo
* 0 Despreciable

En base a lo anteriormente señalado se obtuvieron los siguientes resultados:

|  |  |
| --- | --- |
| [S] Servicios | |
| 01 | Correo electrónico |
| 03 | Mensajería instantánea |

Tabla 3.10 Servicios más valorados.

|  |  |
| --- | --- |
| [D] Datos/Información | |
|  | Plan de contingencia informática |
|  | Programas informáticos diseñados por la Institución |
|  | Respaldos de información |
|  | Base de datos |

Tabla 3.11 Datos/Información más valorados.

|  |  |
| --- | --- |
| [SW] Aplicaciones | |
|  | Windows Server |
|  | Windows XP Profesional |
|  | Linux Centos |
|  | Kaspersky Business Space Security |
|  | SAM (Control de ingresos) |
|  | PFG (Control de archivo y financiero) |
|  | OLYMPO (Control contable y presupuesto) |

Tabla 3.12 Aplicaciones más valoradas.

|  |  |
| --- | --- |
| [HW] Hardware | |
|  | Servidor Principal |
|  | Servidor Financiero |
|  | Servidor Imágenes |
|  | Servidor Control de Antivirus |
|  | Proxy |

Tabla 3.13 Hardware más valorados

|  |  |
| --- | --- |
| [COM] Redes de Comunicación | |
|  | Red interna |

Tabla 3.14 Redes de Comunicación más valorada.

|  |  |
| --- | --- |
| [SI] Soporte de Información | |
|  | Disco duro portable |

Tabla 3.15 Soporte de Información más valorado.

**Identificación de amenazas**

……….

**Desastres naturales**

* Terremoto

**De origen industrial**

* Corte del suministro eléctrico
* Condiciones inadecuadas de temperatura y/o humedad
* Fallo de servicios de comunicaciones
* Degradación de los soportes de almacenamiento de la información

**Errores y fallos no intencionados**

* Errores de los usuarios
* Errores del administrador
* Errores de monitorización (log)
* Errores de configuración
* Errores de re – encaminamiento
* Errores de secuencia
* Escapes de Información
* Alteración de la información
* Introducción de información incorrecta
* Degradación de la información
* Destrucción de información
* Divulgación de información
* Errores de mantenimiento/ actualización de programas (software)
* Errores de mantenimiento/ actualización de equipos (hardware)
* Caída del sistema por agotamiento de recursos
* Indisponibilidad del personal

**Ataques intencionados**

* Abuso de privilegios de acceso
* Uso no previsto
* Difusión de software dañino
* Re- encaminamiento de mensajes
* Alteración de secuencia
* Acceso no autorizado
* Repudio
* Interceptación de información (escucha)
* Modificación de la información
* Introducción de falsa información
* Corrupción de la información
* Destrucción de la información
* Divulgación de información
* Manipulación de programas
* Ataque destructivo
* Ocupación enemiga
* Indisponibilidad del personal
* Extorsión
* Ingeniería social

**Vulnerabilidades y salvaguardas.**

**………..**

**Evaluación del riesgo**

…………

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Correo electrónico | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Caída del sistema por agotamiento de recursos | 7 | 10 | 70 |
| Errores de usuario | 0.08 | 100 | 8 |
| Acceso no autorizado | 0.4 | 10 | 4 |
| Uso no previsto | 0.8 | 1 | 0.8 |
| Repudio | 4 | 0.1 | 0.4 |
| Denegación de servicio | 2 | 0.1 | 0.2 |
| Errores de re – encaminamiento | 0.8 | 0.1 | 0.08 |
| Errores de secuencia | 0.8 | 0.1 | 0.08 |
| Errores de configuración | 0.08 | 0.1 | 0.008 |

Tabla 3.16 Estimación del riesgo. Correo electrónico.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Mensajería instantánea | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| E.1 Errores de usuario | 1 | 10 | 10 |
| Caída del sistema por agotamiento de recursos | 2 | 1 | 2 |
| Repudio | 4 | 0.1 | 0.4 |
| Manipulación de la configuración | 3 | 0.1 | 0.3 |
| Errores del administrador | 2 | 0.1 | 0.2 |
| Errores de configuración | 2 | 0.1 | 0.2 |
| Denegación de servicio | 2 | 0.1 | 0.2 |
| Errores de secuencia | 0.8 | 0.1 | 0.08 |
| Uso no previsto | 0.8 | 0.1 | 0.08 |
| Errores de re – encaminamiento | 0.6 | 0.1 | 0.06 |

Tabla 3.17 Estimación del riesgo. Mensajería instantánea.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Ttransferencia de archivos | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Errores de usuario | 0.6 | 1 | 0.6 |
| Repudio | 4 | 0.1 | 0.4 |
| Errores del administrador | 2 | 0.1 | 0.2 |
| Errores de configuración | 2 | 0.1 | 0.2 |
| Manipulación de la configuración | 2 | 0.1 | 0.2 |
| Errores de secuencia | 1 | 0.1 | 0.1 |
| Caída del sistema por agotamiento de recursos | 0.8 | 0.1 | 0.008 |
| Uso no previsto | 0.8 | 0.1 | 0.008 |
| Errores de re – encaminamiento | 0.6 | 0.1 | 0.006 |

Tabla 3.18 Estimación del riesgo. Transferencia de archivos.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Plan de contingencia informática | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Errores de usuario | 1 | 1 | 1 |
| Escapes de información | 6 | 0.1 | 0.6 |
| Divulgación de información | 5 | 0.1 | 0.5 |
| Alteración de la información | 4 | 0.1 | 0.4 |
| Errores del administrador | 1 | 0.1 | 0.1 |

Tabla 3.19 Estimación del riesgo. Plan de contingencia informática.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Programas informáticos diseñados por la institución | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Errores de usuario | 3 | 10 | 30 |
| Errores del administrador | 4 | 0.1 | 0.4 |
| Errores de configuración | 4 | 0.1 | 0.4 |
| Errores de monitorización (log) | 2 | 0.1 | 0.2 |

Tabla 3.20 Estimación del riesgo. Programas informáticos diseñados por la institución.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Respaldos de información | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Errores de monitorización (log) | 3 | 0.1 | 0.3 |
| Errores de usuario | 2 | 0.1 | 0.2 |
| Errores del administrador | 2 | 0.1 | 0.2 |
| Errores de configuración | 2 | 0.1 | 0.2 |

Tabla 3.21 Estimación del riesgo. Respaldos de información.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Base de datos | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Alteración de la información | 5 | 10 | 50 |
| Introducción de información incorrecta | 5 | 10 | 50 |
| Errores de usuario | 3 | 10 | 30 |
| Destrucción de la información | 8 | 0.1 | 0.8 |
| Destrucción de información | 7 | 0.1 | 0.7 |
| Modificación de la información | 5 | 0.1 | 0.5 |
| Corrupción de la información | 5 | 0.1 | 0.5 |
| Acceso no autorizado | 4 | 0.1 | 0.4 |
| Errores del administrador | 3 | 0.1 | 0.3 |
| Errores de monitorización (log) | 3 | 0.1 | 0.3 |
| Degradación de la información | 0.9 | 0.1 | 0.009 |

Tabla 3.22 Estimación del riesgo. Base de datos.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Windows Server | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Difusión de software dañino | 2 | 1 | 2 |
| Acceso no autorizado | 4 | 0.1 | 0.4 |

Tabla 3.23 Estimación del riesgo. Windows server.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Windows XP Profesional | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Difusión de software dañino | 2 | 10 | 20 |
| Errores de mantenimiento/ actualización de programas (software) | 3 | 0.1 | 0.3 |
| Difusión de software dañino | 2 | 0.1 | 0.2 |

Tabla 3.24 Estimación del riesgo. Windows XP Profesional.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Linux Centos | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Escapes de información | 4 | 0.1 | 0.4 |
| Errores de configuración | 1 | 0.1 | 0.1 |

Tabla 3.25 Estimación del riesgo. Linux centos.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Kaspersky Business Space Security | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Errores de mantenimiento/ actualización de programas (software) | 5 | 1 | 5 |
| vulnerabilidades de los programas (software) | 3 | 1 | 3 |
| Errores de configuración | 2 | 0.1 | 0.2 |

Tabla 3.26 Estimación del riesgo. Kaspersky Business Space Security.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: SAM | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Difusión de software dañino | 3 | 1 | 3 |
| Difusión de software dañino | 3 | 0.1 | 0.3 |
| Acceso no autorizado | 3 | 0.1 | 0.3 |
| Errores de monitorización (log) | 2 | 0.1 | 0.2 |
| Errores de usuario | 0.9 | 0.1 | 0.09 |

Tabla 3.27 Estimación del riesgo. SAM

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: PFG | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Acceso no autorizado | 4 | 0.1 | 0.4 |
| Vulnerabilidades de los programas (software) | 3 | 0.1 | 0.32 |
| Errores de monitorización (log) | 2 | 0.1 | 0.16 |
| Errores de usuario | 0.8 | 0.1 | 0.08 |

Tabla 3.28 Estimación del riesgo. PFG.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: OLYMPO | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Acceso no autorizado | 4 | 0.1 | 0.4 |
| Errores de usuario | 2 | 0.1 | 0.2 |
| Errores de monitorización (log) | 2 | 0.1 | 0.2 |
| Escapes de información | 2 | 0.1 | 0.2 |
| Vulnerabilidades de los programas | 2 | 0.1 | 0.2 |

Tabla 3.29 Estimación del riesgo. OLYMPO.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Servidor Principal | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Corte del suministro eléctrico | 0.8 | 10 | 8 |
| sobrecarga eléctrica | 0.8 | 0.1 | 0.8 |
| Terremoto | 5 | 0.1 | 0.5 |

Tabla 3.30 Estimación del riesgo. Servidor principal.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Servidor Financiero | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Uso no previsto | 6 | 10 | 60 |
| Corte del suministro eléctrico | 0.8 | 10 | 8 |
| Errores de mantenimiento/ actualización de equipos (hardware) | 6 | 1 | 6 |
| Caída del sistema por agotamiento de recursos | 6 | 1 | 6 |
| Denegación de servicio | 5 | 1 | 5 |
| Errores del administrador | 3 | 1 | 3 |
| Acceso no autorizado | 3 | 1 | 3 |
| Sobrecarga eléctrica | 0.8 | 1 | 0.8 |
| Terremoto | 5 | 0.1 | 0.5 |
| Avería de origen físico o lógico | 4 | 0.1 | 0.4 |

Tabla 3.31 Estimación del riesgo. Servidor financiero.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Servidor Proxy | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Corte del suministro eléctrico | 0.8 | 10 | 8 |
| Errores de mantenimiento/ actualización de equipos (hardware) | 6 | 1 | 6 |
| Caída del sistema por agotamiento de recursos | 6 | 1 | 6 |
| Denegación de servicio | 5 | 1 | 5 |
| Acceso no autorizado | 3 | 1 | 3 |
| Sobrecarga eléctrica | 0.8 | 1 | 0.8 |
| Terremoto | 5 | 0.1 | 0.5 |
| Avería de origen físico o lógico | 4 | 0.1 | 0.4 |
| Errores del administrador | 3 | 0.1 | 0.3 |

Tabla 3.32 Estimación del riesgo. Servidor proxy.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Servidor Imágenes | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Corte del suministro eléctrico | 0.8 | 10 | 8 |
| Errores de mantenimiento/ actualización de equipos (hardware) | 5 | 1 | 5 |
| Caída del sistema por agotamiento de recursos | 5 | 1 | 5 |
| Denegación de servicio | 4 | 1 | 4 |
| Acceso no autorizado | 2 | 1 | 2 |
| Terremoto | 5 | 0.1 | 0.5 |
| Avería de origen físico o lógico | 4 | 0.1 | 0.4 |
| Errores del administrador | 3 | 0.1 | 0.3 |
| Sobrecarga eléctrica | 0.8 | 0.1 | 0.08 |

Tabla 3.33 Estimación del riesgo. Servidor imágenes.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Servidor Control de antivirus | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Uso no previsto | 6 | 100 | 600 |
| Corte del suministro eléctrico | 0.8 | 10 | 8 |
| Errores de mantenimiento/ actualización de equipos (hardware) | 6 | 1 | 6 |
| Caída del sistema por agotamiento de recursos | 6 | 1 | 6 |
| Denegación de servicio | 5 | 1 | 5 |
| Acceso no autorizado | 3 | 1 | 3 |
| Sobrecarga eléctrica | 0.8 | 1 | 0.8 |
| Terremoto | 5 | 0.1 | 0.5 |
| Avería de origen físico o lógico | 4 | 0.1 | 0.4 |
| Errores del administrador | 3 | 0.1 | 0.3 |

Tabla 3.34 Estimación del riesgo. Servidor control de antivirus.

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Red Interna | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Avería de origen físico o lógico | 2 | 10 | 20 |
| Fallos de servicios de comunicación | 8 | 1 | 8 |
| Terremoto | 5 | 0.1 | 0.5 |
| Análisis de tráfico | 5 | 0.1 | 0.5 |

Tabla 3.35 Estimación del riesgo. Red interna

|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVO: Disco Duro Portable | | | |
| Amenaza | **Impacto** | **Frecuencia** | **Riesgo** |
| Avería de origen físico o lógico | 3 | 10 | 30 |
| Análisis de tráfico | 0.9 | 1 | 0.9 |
| Terremoto | 5 | 0.1 | 0.5 |
| Fallos de servicios de comunicación | 4 | 0.1 | 0.4 |

Tabla 3.36 Estimación del riesgo. Disco duro portable.

Terminado el análisis de riesgo sobre la Dirección de Sistemas se han identificado los activos con mayor riesgo, valorando los siguientes aspectos:

* activos,
* importancia para la dirección,
* vulnerabilidades que los afectan,
* amenazas que pueden explotar estas vulnerabilidades

**IMPACTO**

Los activos expuestos a mayor impacto, teniendo en cuenta su valor y la degradación que estos sufrirían al ser atacados por las amenazas que los afectan, son los siguientes:

|  |  |
| --- | --- |
| Activos | Impacto |
| [15] Base de Datos | 48,90 |
| [30] Servidor de Control de Antivirus | 39,60 |
| [27] Servidor Financiero | 39,60 |
| [31] Servidor Proxy | 33,60 |
| [29] Servidor de Imagenes | 29,60 |

Tabla 3.37 Activos con mayor impacto.

**RIESGO**

Se obtuvo los activos con mayor riesgo, conociendo su impacto y frecuencia de la ocurrencia de las vulnerabilidades, teniendo la siguiente lista, la cual se trabajará en el Análisis Forense.

|  |  |
| --- | --- |
| Activos | Riesgos |
| [30] Servidor de Control de Antivirus | 630,00 |
| [15] Base de Datos | 133,51 |
| [27] Servidor Financiero | 92,70 |
| [01] Correo Electrónico | 83,57 |

Tabla 3.38 Activos con mayor riesgo.